AUTHENTICATION SYSTEM, PEN-TYPE INPUT DEVICE AND AUTHENTICATION PROCESSING PROGRAM

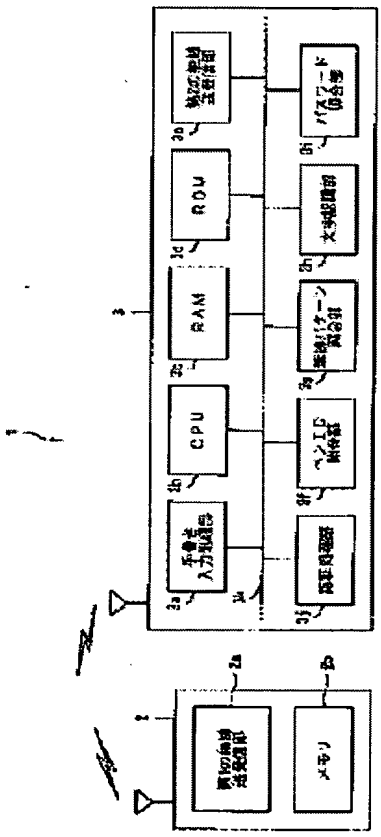
Patent number: JP2003162511
Publication date: 2003-06-06

Inventor: YAMAKADO HITOSHI; MIYAKOSHI DAISUKE; MIYAMOTO TORU
Applicant: SEIKO EPSON CORP

Classification:
- international: G06F15/00; G06K9/62; G06T7/00
- european:
Application number: JP20010357703 20011122
Priority number(s): JP20010357703 20011122

Abstract of **JP2003162511**

<P>PROBLEM TO BE SOLVED: To provide an authentication system making an authentication terminal perform authentication processing necessary, to authenticate handwriting authentication and the like, a pen-type input device for the system and an authentication processing program to control the terminal. <P>SOLUTION: An authentication system 1 comprising a pen-type input device 2 and an authentication terminal 3, wherein the input device 2 comprises a first radio transceiver 2a and a memory 2b storing handwriting authentication data, authentication IDs and password information, the authentication terminal 3 comprises a handwriting input processing part 3a to input authentication information by the input device 2, a second radio transceiver 3e, a pen ID validation part 3f, a character recognition part 3h, handwriting pattern validation part 3g, a password validation part 3i and an authentication processing part 3j, to perform the authentication processing based on the validation results by the password validation part 3i and each validation part 3f, 3g and 3h. <P>COPYRIGHT: (C)2003,JPO



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－162511
（Ｐ２００３－１６２５１１Ａ）
(43)公開日　平成15年６月６日(2003.6.6)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
G06F 15/00	330	G06F 15/00	330	F 5B043
G06K 9/62		G06K 9/62		G 5B064
G06T 7/00	300	G06T 7/00	300	F 5B085
	570		570	5L096

審査請求　未請求　請求項の数12　ＯＬ　（全10頁）

(21)出願番号　特願2001－357703(Ｐ2001－357703)

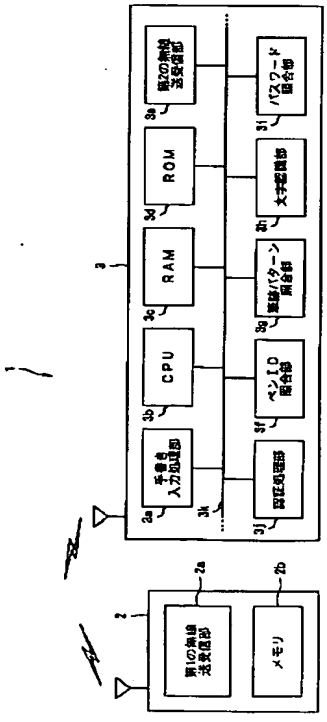
(22)出願日　平成13年11月22日(2001.11.22)

(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(72)発明者　山門　均
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
(72)発明者　宮腰　大輔
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
(74)代理人　100095728
弁理士　上柳　雅誉　（外２名）

最終頁に続く

(54)【発明の名称】認証システム、ペン型入力装置及び認証処理用プログラム

(57)【要約】
【課題】　筆跡鑑定等の認証に必要な認証処理を認証用端末に行わせるペン型入力装置を用いた認証システム、システムにおけるペン型入力装置及び認証用端末を制御するための認証処理用プログラムを提供する。
【解決手段】　認証システム１は、ペン型入力装置２と認証用端末３とから構成され、ペン型入力装置２は、第１の無線送受信部２ａと、筆跡鑑定用データ、認証用ＩＤ及びパスワード情報の記憶されたメモリ２ｂと、を備えた構成とし、認証用端末３は、ペン型入力装置２によって認証情報を入力するため手書き入力処理部３ａと、第２の無線送受信部３ｅと、ペンＩＤ照合部３ｆと、文字認識部３ｈと、筆跡パターン照合部３ｇと、パスワード照合部３ｉと、前記各照合部における照合結果に基づいて認証処理を行う認証処理部３ｊと、を備えた構成とした。



1

【特許請求の範囲】

【請求項１】　ペン型入力装置によって認証用端末に手書きで認証情報を入力するための認証情報入力手段を備え、その入力された認証情報に基づいて入力を行ったシステム利用者の認証を行う認証システムであって、
前記ペン型入力装置は、筆跡鑑定用データを記憶するための鑑定用データ記憶手段と、前記認証用端末に前記筆跡鑑定用データを通知するための鑑定用データ通知手段と、を備え、
前記認証用端末は、前記認証情報が入力されたときに、当該認証情報を解析するための認証情報解析手段と、当該認証情報解析手段の解析結果と前記鑑定用データ通知手段によって通知された前記筆跡鑑定用データとを比較して当該認証情報の筆跡を鑑定する筆跡鑑定手段と、この鑑定結果に基づいて前記システム利用者の認証処理を行う認証手段と、を備えることを特徴とする認証システム。

【請求項２】　前記ペン型入力装置は、自装置を前記認証用端末によって認証するための入力装置認証用データを記憶した入力装置認証用データ記憶手段と、当該入力装置認証用データを前記認証用端末に通知するための入力装置認証用データ通知手段と、を備え、
前記認証用端末は、通知された前記入力装置認証用データに基づいて前記ペン型入力装置を認証する入力装置認証手段を備え、
前記認証手段は、前記入力装置認証手段の認証結果と前記筆跡鑑定手段の鑑定結果とに基づいて前記システム利用者の認証処理を行うようになっていることを特徴とする請求項１記載の認証システム。

【請求項３】　手書き入力される前記認証情報は、前記システム利用者固有のパスワードであり、
前記認証用端末は、手書き入力された前記パスワードの解析結果に基づいて前記パスワードが正しいか否かを判定するパスワード判定手段を備え、
前記認証手段は、前記パスワード判定手段の判定結果にも基づいて前記システム利用者の認証処理を行うようになっていることを特徴とする請求項１又は請求項２記載の認証システム。

【請求項４】　手書き入力される前記認証情報は、前記システム利用者固有のパスワードであり、
前記ペン型入力装置は、前記パスワードを記憶するためのパスワード記憶手段と、当該パスワードを前記認証用端末に通知するためのパスワード通知手段と、を備え、
前記認証手段は、前記パスワード通知手段によって通知された前記パスワードにも基づいて前記システム利用者の認証処理を行うようになっていることを特徴とする請求項１又は請求項２記載の認証システム。

【請求項５】　ペン型入力装置によって認証用端末に手書きで認証情報を入力するための認証情報入力手段を備え、その入力された認証情報に基づいて入力を行ったシステム利用者の認証を行う認証システムにおける前記ペン型入力装置であって、
筆跡鑑定用データを記憶するための鑑定用データ記憶手段と、前記認証用端末に前記筆跡鑑定用データを通知するための鑑定用データ通知手段と、を備えることを特徴とするペン型入力装置。

【請求項６】　自装置を前記認証用端末によって認証するための入力装置認証用データを記憶した入力装置認証用データ記憶手段と、当該入力装置認証用データを前記認証用端末に通知するための入力装置認証用データ通知手段と、を備えることを特徴とする請求項５記載のペン型入力装置。

【請求項７】　手書き入力される前記認証情報は、前記システム利用者固有のパスワードであり、
前記ペン型入力装置は、前記パスワードを記憶するためのパスワード記憶手段と、当該パスワードを前記認証用端末に通知するためのパスワード通知手段と、を備えることを特徴とする請求項５又は請求項６記載のペン型入力装置。

【請求項８】　ペン型入力装置によって認証用端末に手書きで認証情報を入力するための認証情報入力手段を備え、その入力された認証情報に基づいて入力を行ったシステム利用者の認証を行う認証システムにおける前記認証用端末を制御するための認証処理用プログラムであって、
前記認証情報が入力されたときに、当該認証情報を解析するための認証情報解析ステップと、この解析結果とペン型入力装置から通知された前記筆跡鑑定用データとを比較して当該認証情報の筆跡を鑑定する筆跡鑑定ステップと、この鑑定結果に基づいて前記システム利用者の認証処理を行う認証ステップと、を備えることを特徴とする認証処理用プログラム。

【請求項９】　ペン型入力装置によって認証用端末に手書きで認証情報を入力し、その認証情報に基づいて前記入力を行ったシステム利用者の認証を行う認証システムにおける前記認証用端末を制御するための認証処理用プログラムであって、
前記ペン型入力装置によって前記認証用端末に手書きで前記認証情報を入力するための認証情報入力ステップと、前記認証情報が入力されたときに、当該認証情報を解析するための認証情報解析ステップと、この解析結果と前記ペン型入力装置によって通知された前記筆跡鑑定用データとを比較して当該認証情報の筆跡を鑑定する筆跡鑑定ステップと、この鑑定結果に基づいて前記システム利用者の認証処理を行う認証ステップと、を備えることを特徴とする認証処理用プログラム。

【請求項１０】　前記ペン型入力装置から通知された前記入力装置認証用データに基づいて前記ペン型入力装置を認証する入力装置認証ステップを備え、
前記認証ステップにおいては、前記入力装置認証ステッ

プにおける認証結果と前記筆跡鑑定ステップにおける鑑定結果とに基づいて前記システム利用者の認証処理を行うようになっていることを特徴とする請求項８又は請求項９記載の認証処理用プログラム。

【請求項１１】　前記ペン型入力装置によって手書き入力される前記認証情報は、前記システム利用者固有のパスワードであり、

前記認証ステップにおいては、前記ペン型入力装置によって通知された前記パスワードに基づいて前記システム利用者の認証処理を行うようになっていることを特徴とする請求項８乃至請求項１０のいずれかに記載の認証処理用プログラム。

【請求項１２】　前記ペン型入力装置によって手書き入力される前記認証情報は、前記システム利用者固有のパスワードであり、

手書き入力された前記パスワードの解析結果に基づいて前記パスワードが正しいか否かを判定するパスワード判定ステップを備え、

前記認証ステップにおいては、前記パスワード判定ステップにおける判定結果に基づいて前記システム利用者の認証処理を行うようになっていることを特徴とする請求項８乃至請求項１０のいずれかに記載の認証処理用プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報端末機器等の利用者の認証を行うための認証システムに係り、特に、手書きで入力された認証情報に基づいて利用者の認証処理を行うのに好適な認証システム、システムにおけるペン型入力装置及び認証用端末を制御するための認証処理用プログラムに関する。

【０００２】

【従来の技術】従来、ペン型入力装置を利用した個人の認証システムとして、特開平１０－２２２２４１号公報に記載された電子ペンを利用した個人認証システムがある。これは、コンピュータ入力装置として使用され署名を行った個人を認証する電子ペンを用いてコンピュータ使用を所望する個人を認証するシステムであって、電子ペンには、署名特徴データを記憶した署名特徴記憶手段と、署名特徴データと電子ペン署名結果との比較に基づき個人を認証する認証手段とが備わっており、認証された個人に対してコンピュータの使用を許可するものである。

【０００３】

【発明が解決しようとする課題】しかしながら、上記従来の認証システムにおいては、署名による筆跡の鑑定を、電子ペン側で行っているので、署名された文字を認識する処理などの多くの計算処理を行うため携帯型機器である電子ペンに搭載される小型のＣＰＵでは処理に時間がかかる恐れがある。また、そのために、複雑な認証処理を行わせることが困難である。

【０００４】そこで、本発明は、このような従来の技術の有する未解決の課題に着目してなされたものであって、筆跡鑑定等の認証に必要な認証処理を認証用端末に行わせるペン型入力装置を用いた認証システム、システムにおけるペン型入力装置及び認証用端末を制御するための認証処理用プログラムを提供することを目的としている。

【０００５】

【課題を解決するための手段】上記目的を達成するために、本発明に係る請求項１記載の認証システムは、ペン型入力装置によって認証用端末に手書きで認証情報を入力するための認証情報入力手段を備え、その入力された認証情報に基づいて入力を行ったシステム利用者の認証を行う認証システムであって、前記ペン型入力装置は、筆跡鑑定用データを記憶するための鑑定用データ記憶手段と、前記認証用端末に前記筆跡鑑定用データを通知するための鑑定用データ通知手段と、を備え、前記認証用端末は、前記認証情報が入力されたときに、当該認証情報を解析するための認証情報解析手段と、当該認証情報解析手段の解析結果と前記鑑定用データ通知手段によって通知された前記筆跡鑑定用データとを比較して当該認証情報の筆跡を鑑定する筆跡鑑定手段と、この鑑定結果に基づいて前記システム利用者の認証処理を行う認証手段と、を備えることを特徴としている。

【０００６】このような構成であれば、ペン型入力装置は、鑑定用データ記憶手段によって記憶された筆跡鑑定用データを鑑定用データ通知手段によって、認証用端末に伝送し、更に、認証情報入力手段によって、認証用端末に手書きで認証情報を入力することが可能である。更に、認証用端末は、認証情報が手書き入力されると、認証情報解析手段によって入力内容を解析し、この解析結果と通知された筆跡鑑定用データとに基づいて筆跡鑑定手段によって、筆跡を鑑定し、この鑑定結果に基づいて認証手段によって認証処理を行うことが可能である。

【０００７】従って、ペン型入力装置は、例えば、その使用者の筆跡鑑定用データを鑑定用データ記憶手段によって記憶しておき、そのデータを鑑定用データ通知手段によって認証用端末に通知し、認証用端末側で、認証情報の解析、筆跡の鑑定及び認証処理を行うので、ペン型入力装置側は、筆跡鑑定用データを通知する処理を行うだけで良く、ペン型入力装置に搭載するＣＰＵは比較的低機能なもので良く、コストの低減に役立つ。

【０００８】また、請求項２に係る発明は、請求項１記載の認証システムにおいて、前記ペン型入力装置は、自装置を前記認証用端末によって認証するための入力装置認証用データを記憶した入力装置認証用データ記憶手段と、当該入力装置認証用データを前記認証用端末に通知するための入力装置認証用データ通知手段と、を備え、前記認証用端末は、通知された前記入力装置認証用デー

タに基づいて前記ペン型入力装置を認証する入力装置認証手段を備え、前記認証手段は、前記入力装置認証手段の認証結果と前記筆跡鑑定手段の鑑定結果とに基づいて前記システム利用者の認証処理を行うようになっていることを特徴としている。

【０００９】つまり、ペン型入力装置は、筆跡鑑定用データに加え、入力装置認証用データ記憶手段によって入力装置認証用データを記憶し、入力装置認証用データ通知手段によって、認証用端末に入力装置認証用データを通知し、一方、認証用端末は、入力装置認証用データを取得すると、このデータに基づいて入力装置認証手段によって入力装置自体の認証を行うようになっている。そして、認証手段は、入力装置の認証結果にも基づいて認証処理を行う。

【００１０】従って、筆跡鑑定に加え、ペン型入力装置自体の認証も行うので、利用者を制限するようなシステムにおいてセキュリティが強化され、システムの安全性が増加する。また、請求項３に係る発明は、請求項１又は請求項２記載の認証システムにおいて、手書き入力される前記認証情報は、前記システム利用者固有のパスワードであり、前記認証用端末は、手書き入力された前記パスワードの解析結果に基づいて前記パスワードが正しいか否かを判定するパスワード判定手段を備え、前記認証手段は、前記パスワード判定手段の判定結果に基づいて前記システム利用者の認証処理を行うようになっていることを特徴としている。

【００１１】つまり、手書き入力される認証情報がシステム利用者固有のパスワードである場合であり、認証用端末は、パスワードが入力されると、パスワード判定手段によって、そのパスワードが正しいか否かを判定し、認証手段は、その判定結果にも基づいて認証処理を行うようになっている。従って、筆跡鑑定に加え、パスワードによる認証も行われるので、利用者を制限するようなシステムにおいてセキュリティが強化され、システムの安全性が増加する。

【００１２】また、請求項４に係る発明は、請求項１又は請求項２記載の認証システムにおいて、手書き入力される前記認証情報は、前記システム利用者固有のパスワードであり、前記ペン型入力装置は、前記パスワードを記憶するためのパスワード記憶手段と、当該パスワードを前記認証用端末に通知するためのパスワード通知手段と、を備え、前記認証手段は、前記パスワード通知手段によって通知された前記パスワードにも基づいて前記システム利用者の認証処理を行うようになっていることを特徴としている。

【００１３】つまり、手書き入力する認証情報がシステム利用者固有のパスワードである場合であり、ペン型入力装置は、パスワード記憶手段によってパスワードを記憶し、パスワード通知手段によって認証用端末にパスワードを通知するようになっており、一方、認証用端末は、パスワードを取得すると、認証手段によって、そのパスワードにも基づいて認証処理を行うようになっている。

【００１４】従って、筆跡鑑定に加え、パスワードによる認証も行われるので、利用者を制限するようなシステムにおいてセキュリティが強化され、更に、パスワードの情報はペン型入力装置側に記憶されているので、他人のパスワードを利用されにくくなり、システムの安全性が向上する。また、本発明に係る請求項５記載のペン型入力装置は、ペン型入力装置によって認証用端末に手書きで認証情報を入力するための認証情報入力手段を備え、その入力された認証情報に基づいて入力を行ったシステム利用者の認証を行う認証システムにおける前記ペン型入力装置であって、筆跡鑑定用データを記憶するための鑑定用データ記憶手段と、前記認証用端末に前記筆跡鑑定用データを通知するための鑑定用データ通知手段と、を備えることを特徴としている。

【００１５】また、請求項６に係る発明は、請求項５記載のペン型入力装置において、自装置を前記認証用端末によって認証するための入力装置認証用データを記憶した入力装置認証用データ記憶手段と、当該入力装置認証用データを前記認証用端末に通知するための入力装置認証用データ通知手段と、を備えることを特徴としている。

【００１６】また、請求項７に係る発明は、請求項５又は請求項６記載のペン型入力装置において、手書き入力される前記認証情報は、前記システム利用者固有のパスワードであり、前記ペン型入力装置は、前記パスワードを記憶するためのパスワード記憶手段と、当該パスワードを前記認証用端末に通知するためのパスワード通知手段と、を備えることを特徴としている。

【００１７】ここで、請求項５乃至請求項７に記載のペン型入力装置は、請求項１乃至請求項４記載の認証システムにおいて使用されるものであり、その作用効果は同様のものとなるので記載を省略する。また、本発明に係る請求項８記載の認証処理用プログラムは、ペン型入力装置によって認証用端末に手書きで認証情報を入力するための認証情報入力手段を備え、その入力された認証情報に基づいて入力を行ったシステム利用者の認証を行う認証システムにおける前記認証用端末を制御するための認証処理用プログラムであって、前記認証情報が入力されたときに、当該認証情報を解析するための認証情報解析ステップと、この解析結果とペン型入力装置から通知された前記筆跡鑑定用データとを比較して当該認証情報の筆跡を鑑定する筆跡鑑定ステップと、この鑑定結果に基づいて前記システム利用者の認証処理を行う認証ステップと、を備えることを特徴としている。

【００１８】また、請求項９に係る発明は、請求項８記載の認証処理用プログラムにおいて、ペン型入力装置によって認証用端末に手書きで認証情報を入力し、その認

証情報に基づいて前記入力を行ったシステム利用者の認証を行う認証システムにおける前記認証用端末を制御するための認証処理用プログラムであって、前記ペン型入力装置によって前記認証用端末に手書きで前記認証情報を入力するための認証情報入力ステップと、前記認証情報が入力されたときに、当該認証情報を解析するための認証情報解析ステップと、この解析結果と前記ペン型入力装置によって通知された前記筆跡鑑定用データとを比較して当該認証情報の筆跡を鑑定する筆跡鑑定ステップと、この鑑定結果に基づいて前記システム利用者の認証処理を行う認証ステップと、を備えることを特徴としている。

【００１９】また、請求項１０に係る発明は、請求項８又は請求項９記載の認証処理用プログラムにおいて、前記ペン型入力装置から通知された前記入力装置認証用データに基づいて前記ペン型入力装置を認証する入力装置認証ステップを備え、前記認証ステップにおいては、前記入力装置認証ステップにおける認証結果と前記筆跡鑑定ステップにおける鑑定結果とに基づいて前記システム利用者の認証処理を行うようになっていることを特徴としている。

【００２０】また、請求項１１に係る発明は、請求項８乃至請求項１０のいずれかに記載の認証処理用プログラムにおいて、前記ペン型入力装置によって手書き入力される前記認証情報は、前記システム利用者固有のパスワードであり、前記認証ステップにおいては、前記ペン型入力装置によって通知された前記パスワードに基づいて前記システム利用者の認証処理を行うようになっていることを特徴としている。

【００２１】また、請求項１２に係る発明は、請求項８乃至請求項１０にいずれかに記載の認証処理用プログラムにおいて、前記ペン型入力装置によって手書き入力される前記認証情報は、前記システム利用者固有のパスワードであり、手書き入力された前記パスワードの解析結果に基づいて前記パスワードが正しいか否かを判定するパスワード判定ステップを備え、前記認証ステップにおいては、前記パスワード判定ステップにおける判定結果に基づいて前記システム利用者の認証処理を行うようになっていることを特徴としている。

【００２２】ここで、請求項８乃至請求項１２記載の認証処理用プログラムは、請求項１乃至請求項４記載の認証システムにおける認証用端末を制御するためのプログラムであり、その効果は同様のものとなるので記載を省略する。

【００２３】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて説明する。図１乃至図４は、本発明に係る認証システムの実施の形態を示す図である。まず、本発明に係る認証システムの構成を図１に基づいて説明する。図１は、本発明に係る認証システムの構成を示すブロック図である。

【００２４】認証システム１は、ペン型入力装置２と、認証用端末３と、から構成される。ペン型入力装置２は、認証用端末３との間で無線でデータの送受信を行うための第１の無線送受信部２ａと、手書き文字を認証するための筆跡鑑定用データ、ペン型入力装置２自体を認証するための認証用ＩＤ及びパスワード情報の記憶されたメモリ２ｂと、を備えた構成となる。

【００２５】認証用端末３は、表示部を有するＰＣ（Personal Computer）やＰＤＡ（Personal Digital Assistant）等の情報端末機器であり、ペン型入力装置２によって表示部上に手書きで認証情報を入力するため手書き入力処理部３ａと、認証処理用のプログラムを実行し各部の処理を行うためのＣＰＵ３ｂと、プログラムの実行に必要なデータを一時記憶するためのＲＡＭ３ｃと、認証処理用のプログラムの記憶されたＲＯＭ３ｄと、ペン型入力装置との間のデータ通信を無線で行うための第２の無線送受信部３ｅと、受信したペン型入力装置２の認証用ＩＤが正しいＩＤであるか否かを判定処理するためのペンＩＤ照合部３ｆと、表示部を介して手書き入力された認証情報を解析して文字として認識するための文字認識部３ｈと、入力された文字パターンとペン型入力装置２から受信した筆跡鑑定用データとに基づいて、入力された文字データがペン型入力装置２の利用者のものと一致するか否かを判定する筆跡パターン照合部３ｇと、文字認識部３ｈによって認識された文字とペン型入力装置２から受信したパスワード情報と図示しないパスワード照合用データベースの登録内容とに基づいて入力された認証情報であるパスワードが正しいものであるか否かを判定するめのパスワード照合部３ｉと、前記各照合部における照合結果に基づいて認証処理を行う認証処理部３ｊと、これらＣＰＵ、メモリ及び各部間のデータの送受信を行うためのバス３ｋと、を備えた構成となる。

【００２６】具体的な動作を図２に基づいて説明する。図２は、ペン型入力装置２によって、認証情報を手書きで行う一例を示す図である。図２に示すように、認証システム１においては、認証用端末３の表示部３ａ’にペン型入力装置２によって認証情報を手書きで入力することになる。ここで、本実施の形態においては、表示部３ａ’は、タッチパネルとなっており、これにより、手書き入力処理部３ａは、ペン先の接触した座標情報を取得して認証情報の描画処理を行う。描画結果の情報は、文字認識部３ｈ、筆跡パターン照合部３ｇ及びパスワード照合部３ｉへと伝送され、そこで、認識処理又は照合処理が行われる。また、手書き入力が行われる前に、認証用端末からの要求に応じてペン型入力装置２の備える第１の無線送受信部２ａによって、メモリ２ｂから読み出された筆跡鑑定用データ、認証用ＩＤ及びパスワード情報が認証用端末３に伝送される。そして、伝送された各情報は、認証用端末３の備える第２の無線送受信部３ｅ

によって受信され、各照合部へと伝送される。従って、ペンＩＤ照合部３ｆでは、取得した認証用ＩＤに基づいてＩＤが正しいか否かを判定し、筆跡パターン照合部３ｇでは、取得した筆跡鑑定用データに基づいて筆跡パターンが利用者のものと一致するか否かを判定し、パスワード照合部３ｉでは、取得したパスワード情報に基づいてペン型入力装置２に記憶されたパスワード情報及び入力されたパスワードが正しいものであるか否かを判定する処理を行う。ここで、パスワード照合における判定処理を行うために、手書き入力された認証情報（ここではパスワード）は、文字認識部３ｈにおいて、認識処理が行われる。これにより入力された情報は文字情報に変換され、パスワード照合部３ｉにおける照合処理が可能となる。更に、各照合部における処理が終了するとそれら処理結果は、認証処理部３ｊに伝送され、取得した処理結果に基づいて認証処理が行われる。

【００２７】次に、認証システム１におけるペン型入力装置２の処理の流れを図３に基づいて説明する。図３は、認証システム１におけるペン型入力装置２の処理を示すフローチャートである。図３に示すように、まず、ステップＳ３００に移行し、第１の無線送受信部２ａによって、認証用端末３に認証要求信号を送信してステップＳ３０２に移行する。

【００２８】ステップＳ３０２では、認証用ＩＤの要求信号を受信したか否かを判定し、受信したと判定した場合（Yes)は、ステップＳ３０４に移行し、そうでない場合(No)は受信するまで待機する。ステップＳ３０４に移行した場合は、メモリ２ｂから認証用ＩＤを読み出してステップＳ３０６に移行する。

【００２９】ステップＳ３０６では、第１の無線送受信部２ａによって、読み出された認証用ＩＤを送信しステップＳ３０８に移行する。ステップＳ３０８では、パスワード情報の要求信号を受信したか否かを判定し、受信したと判定された場合(Yes)はステップＳ３１０に移行し、そうでない場合(No)は受信するまで待機する。

【００３０】ステップＳ３１０に移行した場合は、メモリ２ｂからパスワード情報を読み出してステップＳ３１２に移行する。ステップＳ３１２では、第１の無線送受信部２ａによって、読み出されたパスワード情報を送信してステップＳ３１４に移行する。ステップＳ３１４に移行すると、筆跡鑑定用データの要求信号を受信したか否かを判定し、受信したと判定した場合(Yes)はステップＳ３１６に移行し、そうでない場合(No)は受信するまで待機する。

【００３１】ステップＳ３１６に移行した場合は、メモリ２ｂから筆跡鑑定用データを読み出してステップＳ３１８に移行する。ステップＳ３１８では、第１の無線送受信部２ａによって、読み出された筆跡鑑定用データを送信して処理を終了する。更に、認証システム１における認証用端末３の処理の流れを図４に基づいて説明する。図４は、認証システム１における認証用端末３の処理を示すフローチャートである。

【００３２】図４に示すように、まずステップＳ４００に移行し、ペン型入力装置２から認証要求信号を受信したか否かを判定し、受信したと判定した場合(Yes)はステップＳ４０２に移行し、そうでない場合(No)は受信するまで待機する。ステップＳ４０２に移行した場合は、第２の送受信部３ｅによって、ペン型入力装置２に認証用ＩＤの送信要求信号を送信してステップＳ４０４に移行する。

【００３３】ステップＳ４０４では、ペン型入力装置２から認証用ＩＤを受信したか否かを判定し受信したと判定した場合(Yes)はステップＳ４０６に移行し、そうで無い場合(No)は受信するまで待機する。このとき、認証用ＩＤが受信されない時間が一定時間を超えるような場合にはステップＳ４０２に移行して、認証用ＩＤの送信要求信号を再送する処理を行うようにしても良い。

【００３４】ステップＳ４０６に移行した場合は、ペンＩＤ照合部３ｆにおいて、取得した認証用ＩＤが図示しない認証用ＩＤ登録データベースに登録されたＩＤか否かを判定するための照合処理を行いステップＳ４０８に移行する。ステップＳ４０８では、照合結果に基づいて取得した認証用ＩＤが登録されたものか否かを判定し、登録されたものである場合(Yes)はステップＳ４１０に移行し、そうでない場合(No)はステップＳ４００に移行する。

【００３５】ステップＳ４１０に移行した場合は、判定結果を認証処理部３ｊに伝送してステップ４１２に移行する。ステップＳ４１２では、第２の送受信部によって、パスワード情報要求信号をペン型入力装置２に伝送してステップＳ４１４に移行する。ステップＳ４１４では、ペン型入力装置２からパスワード情報を受信したか否かを判定し、受信したと判定した場合(Yes)はステップＳ４１６に移行し、そうでない場合(No)はパスワード情報を受信するまで待機する。このとき、パスワード情報が受信されない時間が一定時間を超えるような場合にはステップＳ４１２に移行してパスワード情報要求信号を送信する処理を行うか、ステップＳ４０２に移行して、認証用ＩＤの送信要求信号を送信する処理を行うようにしても良い。

【００３６】ステップＳ４１６に移行した場合は、第２の送受信部３ｅによって、筆跡鑑定用データ受信要求信号をペン型入力装置２に伝送してステップＳ４１８に移行する。ステップＳ４１８では、ペン型入力装置２から筆跡鑑定用データを受信したか否かを判定し、受信したと判定した場合(Yes)はステップＳ４２０に移行し、そうでない場合(No)は筆跡鑑定用データを受信するまで待機する。このとき、筆跡鑑定用データが受信されない時間が一定時間を超えるような場合にはステップＳ４１６に移行して筆跡鑑定用データ要求信号を送信する処理を

行うか、ステップＳ４０２に移行して、認証用ＩＤの送信要求信号を送信する処理を行うようにしても良い。

【００３７】ステップＳ４２０に移行した場合は、認証情報の手書き入力を要求するメッセージを表示部に表示してステップＳ４２２に移行する。ステップＳ４２２に移行すると、ペン型入力装置２によって、認証情報（パスワードと同一）が入力されたか否かを判定し、入力されたと判定された場合(Yes)はステップＳ４２４に移行し、そうでない場合(No)は認証情報が入力されるまで待機する。

【００３８】ステップＳ４２４に移行した場合は、文字認識部３ｈによって、手書き入力された認証情報を文字認識処理し、パスワード照合部３ｉによって認識された文字情報及び取得したパスワード情報が図示しないパスワード情報登録データベースに登録されたものと一致するか否かを判定するための照合処理を行い、筆跡パターン照合部では、取得した筆跡鑑定用データに基づいて認証情報の入力者を特定するための筆跡鑑定処理を行い、ステップＳ４２６に移行する。

【００３９】ここで、本実施の形態における筆跡鑑定処理は、「文字の形態に関する事項」、「送筆、運筆に関する事項」の２つの項目に対して、入力時のデータとペン型入力装置２から取得した入力者固有の筆跡鑑定用データとを比較することで行う。つまり、手書きされた文字が漢字であれば、撥ねや払いなどの形状が入力者本人のものと同様のものであるか否かを判定したり、漢字の書き順などの文字入力時の描画パターンなどが本人と一致する否かなどを判定したりする。従って、筆跡鑑定用データには、入力者固有の文字の形態や描画時のパターンなどの情報が含まれている。

【００４０】ステップＳ４２６に移行すると、これらの処理結果を認証処理部３ｊに伝送してステップＳ４２８に移行する。ステップＳ４２８に移行すると、認証処理部３ｊによって、取得した処理結果に基づいて、認証情報の入力者の認証処理を行い一連の処理を終了する。ここで、本実施の形態においては、ペン型入力装置２自体が記憶保持している、パスワード情報及び認証用ＩＤが認証用端末３側に登録されたものであり、且つ、手書き入力されたパスワードが適切な入力者のものであると判定された場合のみに、入力者を認証することになる。

【００４１】以上、上記実施の形態によれば、ペン型入力装置２によって、認証用端末３の表示部を介して認証情報を手書きで入力すると、認証用端末３側で認証処理を行うようになっているので、ペン側に高機能なＣＰＵを搭載する必要が無くコストの低減が望める。また、ペン型入力装置２に筆跡鑑定用データ、パスワード情報及びペン型入力装置２の認証用ＩＤを記憶しておき、これらのデータを認証用端末３からの要求信号に応じて伝送し、認証用端末３は、取得した情報に基づいて認証処理を行うようになっているので、認証情報入力者の認証をより確実に行うことが可能となるので、セキュリティの向上に役立つ。

【００４２】なお、この認証システムは、端末機器やアプリケーションソフトなどの利用制限を行う場合や、他のシステムにおいて利用者の承認を行う場合などに適用されるものであり、特に、利用者の認証を厳密に行うことが可能なため、承認処理等の重要な処理が必要なシステムに適している。従って、例えば、オンライン決算システムにおける承認処理やＣＡＤ（Computer Aided Design）などによる図面改編時の改編者の特定などを容易に行うことが可能である。

【００４３】ここで、図１に示す、手書き入力処理部３ａは、請求項１記載の認証情報入力手段に対応し、メモリ２ｂは、請求項１、２、４、５、６、７記載の鑑定用データ記憶手段、入力装置認証用データ記憶手段及びパスワード記憶手段に対応し、第１の無線送受信部２ａは、請求項１、２、４、５、６、７記載の鑑定用データ通知手段、入力装置認証用データ通知手段及びパスワード通知手段に対応し、筆跡パターン照合部３ｇは、請求項１記載の認証情報解析手段及び筆跡鑑定手段に対応し、ペンＩＤ照合部３ｆは、請求項２記載の入力装置認証手段に対応し、パスワード照合部３ｉは、請求項３記載のパスワード判定手段に対応し、認証処理部３ｊは、請求項１記載の認証手段に対応する。

【００４４】なお、上記実施の形態においては、手書き入力する認証情報をパスワードと同一のものとしているが、これに限らず、入力者の名前を漢字で入力したり、図形を入力したりするなど、どのようなものを認証情報として入力するようにしても良い。また、上記実施の形態においては、ペン型入力装置２及び認証用端末３の処理は、各要求信号に応じて行われるようになっているが、これに限らず、ペン型入力装置２と認証用端末３との間の通信状態が確立した後に、データ送受信及び認証処理を行うようにするなど、どのような処理方法で行うようにしても良い。

【００４５】また、上記実施の形態においては、認証用端末３は、ペン型入力装置２から認証用ＩＤ、入力パスワード情報及び筆跡鑑定用データの３種類の認証処理用のデータを受信し、それらのデータに基づいて認証処理を行うようにしているが、これに限らず、筆跡鑑定用データだけを受信して、このデータと手書き入力されたデータとに基づいて認証処理を行うようにしたり、認証用ＩＤ及び筆跡鑑定用データの２種類のデータを受信して、これらのデータに基づいて認証処理を行うようにしたり、ペン型入力装置２側にパスワード情報を記憶させず、パスワード情報は認証端末３側のみが持つようにして、認証情報としてパスワードを手書き入力して、筆跡鑑定用データに加えパスワードの確認も含む認証処理を行うようにしたりするなど、どのような組み合わせや方法で行うようにしても良い。

【００４６】また、上記実施の形態においては、筆跡鑑定用データの他に、ペン型入力装置２自体を認証するための認証用ＩＤと、パスワード情報とを加えて認証処理を行っているが、これに限らず、本発明の趣旨に逸脱しない範囲でどのようなデータと組み合わせて認証処理を行うようにしても良い。

【００４７】

【発明の効果】以上説明したように、本発明に係る請求項１記載の認証システムによれば、ペン型入力装置は、例えば、その使用者の筆跡鑑定用データを鑑定用データ記憶手段によって記憶しておき、そのデータを鑑定用データ通知手段によって認証用端末に通知し、認証用端末側で、認証情報の解析、筆跡の鑑定及び認証処理を行うので、ペン型入力装置側は、筆跡鑑定用データを通知する処理を行うだけで良く、ペン型入力装置に搭載するＣＰＵは比較的低機能なもので良く、コストの低減に役立つ。

【００４８】また、請求項２記載の認証システムによれば、筆跡鑑定に加え、ペン型入力装置自体の認証も行うので、利用者を制限するようなシステムにおいてセキュリティが強化され、システムの安全性が増加する。また、請求項３記載の認証システムによれば、筆跡鑑定に加え、パスワードによる認証も行われるので、利用者を制限するようなシステムにおいてセキュリティが強化され、システムの安全性が増加する。

【００４９】また、請求項４記載の認証システムによれば、筆跡鑑定に加え、パスワードによる認証も行われるので、利用者を制限するようなシステムにおいてセキュリティが強化され、更に、パスワードの情報はペン型入力装置側に記憶されているので、他人のパスワードを利用されにくくなり、システムの安全性が向上する。

【図面の簡単な説明】

【図１】本発明に係る認証システムの構成を示すブロック図である。

【図２】ペン型入力装置２によって、認証情報を手書きで行う一例を示す図である。

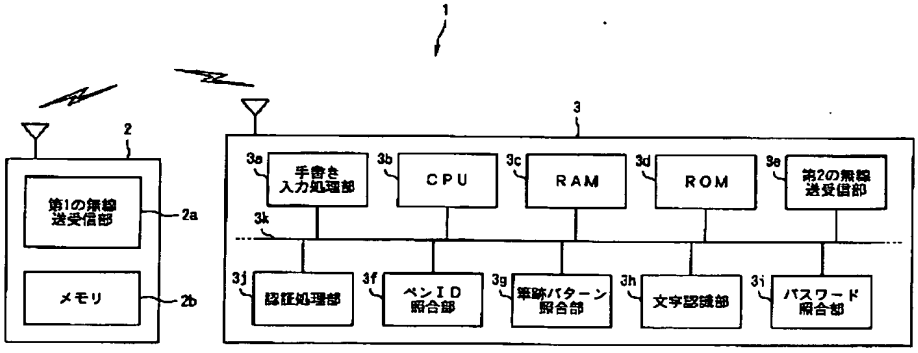
【図３】認証システム１におけるペン型入力装置２の処理を示すフローチャートである。

【図４】認証システム１における認証用端末３の処理を示すフローチャートである。

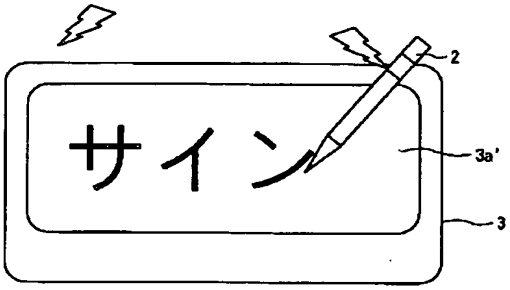
【符号の説明】

１	認証システム
２	ペン型入力装置
２ａ	第１の無線送受信部
２ｂ	メモリ
３	認証用端末
３ａ	手書き入力処理部
３ｆ	ペンＩＤ照合部
３ｇ	筆跡パターン照合部
３ｉ	パスワード照合部
３ｊ	認証処理部

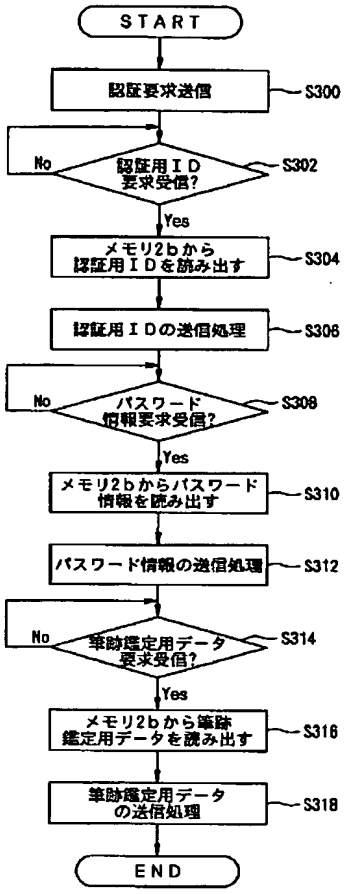
【図１】



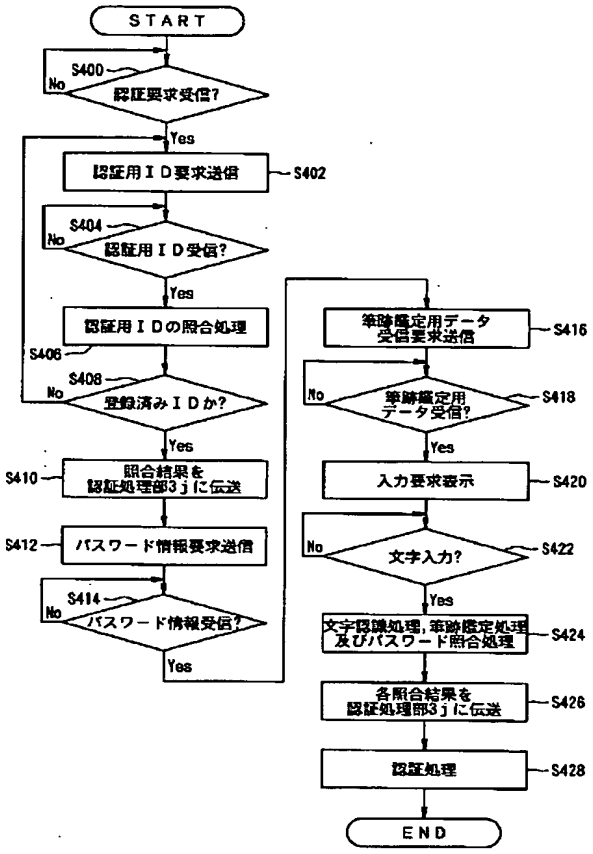
【図２】


サイン
2
3a'
3

【図３】


START
認証要求送信
S300
No
認証用ＩＤ要求受信?
S302
Yes
メモリ2bから認証用ＩＤを読み出す
S304
認証用ＩＤの送信処理
S306
No
パスワード情報要求受信?
S308
Yes
メモリ2bからパスワード情報を読み出す
S310
パスワード情報の送信処理
S312
No
筆跡鑑定用データ要求受信?
S314
Yes
メモリ2bから筆跡鑑定用データを読み出す
S316
筆跡鑑定用データの送信処理
S318
END

【図４】



フロントページの続き

(72)発明者　宮本　徹
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

Ｆターム(参考)　5B043 AA04 BA06 DA07 FA03 GA02
5B064 AB04 BA05 FA18
5B085 AA08 AE02 AE15 BE01
5L096 BA17 CA27 DA02 FA51 HA07
JA11